People Centred Information Security Model for Corporate Nigeria

Fidelis O. Aghware, *Member, IAENG* and Emeka O. Egbuna

***Abstract* - Information and Communication Technology (ICT) has become an agent of change in this 21st century. The deployment of information and communication technologies in tackling national issues has manifested a great profit in notable areas of human endeavor and national economies. However, in some other areas the trend has been dared by numerous fast growing socio - economic challenges infringing unexpectedly on the Nations' information security. This paper therefore addresses the people issues affecting Information Security (IS) in organizations and corporate bodies (CB), and discusses the critical business needs for security; a comprehensive view of the ecological security risks and human related security threats; a discussion of the consequences of human neglect for security; a discussion of recommended security strategies; descriptive-interpretative data revealing security professionals' perceptions about organizational security issue. In this paper, a people centered Information security model is designed using American Encryption Standard for sending messaging/information across networks.**

***Index Terms* - National security, information and communication technology, corporate nation, Information security model**

I. INTRODUCTION

The emergency and development of technology in the 21st century has been warmly welcomed globally. This is in relation to the efficiencies and diverse benefits arising from the technological advancements in the human society and more so in the corporate sector. For instance, the Information Technology sector has been the key beneficiary of advancement in technology, whereby provision and processing of information through the use of sophisticated technology has been made possible. Nevertheless, the development in technology in the information sector has not been exempted from limitations. This is specifically in the issues of security, whereby technology has been dishonestly abused by different persons or institutions at the expense of other people or institutions. Organized criminal activities in the information sector have been in the increase in recent days, which leads to breaking into personal or organizational data environment for malicious motives. The proliferation of hackers and the threats they pose to national security and the global economy have captured the attention of the authorities, business communities and the media all over the world.

Manuscript received August 07, 2012; revised August 08, 2012.

F. O. Aghware is a Reader with College of Education, Agbor, Delta State, Nigeria. He is also a member of Nigeria Computer Society and Computer Professionals Registration Council of Nigeria. (+2348033458475, aghwarefo@yahoo.com)

E. O. Egbuna is a lecturer with College of Education, Agbor, Delta State, Nigeria.

On the economic front, a recent study commissioned by PriceWaterhouseCoopers involving 4,900 IT professionals in 30 different countries indicated that corporate hacking is estimated to cost the world economy an astounding US$1.6 trillion in the year 2000 [1]. In fact, the latest "2002 Computer Crime and Security Survey" jointly conducted by Computer Security Institute (CSI) and Federal Bureau of Investigation (FBI) points toward an upward trend in security risks to U.S. organizations [2]. Many businesses have been in the outcry for insecurity in their information data environment, thus leading to severe loses and unfavorable business environment. Based on this situation, this paper has been mainly focused at providing a root cause analysis on information security roadmap as well as providing long term solutions for modeling the information security roadmap. This is in response to the diverse challenges faced by the corporate society through poor information security roadmaps.

II. INFORMATION SECURITY

Information security is an act of protecting your data away from unauthorized access. It involves data privacy and also comprises of activities like protecting the data away from unauthorized disclosure, destruction, disruption or modification [3].

There is a rapid increase in the number of people that are using the network and internet today exchanging information over the Internet; this has led to a diminishing value of their transactions over electronic networks. Security of information is a critical issue that cannot be overlooked at a go hence there is the need to lay out a model that will cater for effective transfer and sharing of information over electronic networks. In corporate Nigeria for example, people should be a policy guiding information security so as to keep private information confidential and secured.

Security breaches have become a key challenge in policy making thus making it difficult to meet an adequate policy response for securing information especially on the network hence making it a complex task. In a country like Nigeria there is the need to put several legal measures in place with specific implication on information security appropriate to the involved risks. In corporate Nigeria for example, people should be a policy guiding information security so as to keep private information confidential and secured. For instance, authentications which will need the confirmation of certain identities or entries, proper authentication methods are needed for many applications and services [4]. These services or applications may include concluding a contract online or controlling access to certain data and authentication of websites. Other data characteristic is integrity which shows that the information sent has been received unchanged without any alterations whatsoever.

ISBN: 978-988-19251-6-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

More so, information sent may include files that are confidential and may not be needed to be shared by unauthorized access. This is needed especially when you are transferring sensitive information [5]. We need to look at all aspects that threaten security, not just the ones that have malicious intent.

Corporate Nigeria is more of a business organization with an objective of mainly encouraging business in Nigeria. Its main agenda is fundamental in the fields of commerce, business, investment and trade. For such an organization to prosper the flow of information is vital both at an international level and a local level. To achieve this goal however the organization has to get access to a network or the internet for the purposes of advertising and making public its criteria known to the general public and the global community in the fields of commerce, trade, business and investment. With the free flow of information the organization is exposed both to potential hackers, competitive businesses and malicious organizations which can easily bring the company down [5].

III. THE HUMAN ISSUE

Information from the various detailed researches shows that technology has been given more attention than the end users - the people who manage the information. This is because, in the early days of the information revolution, information security as a discipline focused more on protection of classified information stored on operating systems. However, recent researches have shown that so much of the security of data and information is hinged on the human factor [6] and according to [7], people are still the weakest security link in information management and must be considered a very strong factor. This view is been strongly supported by [26], [27] and [8] all of whom are well respected security practitioner. It is vital therefore to focus on the human psychology in attempting to win the security race rather than seeing security as purely technological issue in many organizations.

IV. THE POLICY ISSUE

Information security matters have become an integral part of organisations, business communities, security industry experts and researchers as they need to ensure that they are adequately protected against the threats and risk over the proliferation of hackers and their negative social and economic impacts. Whilst legislatures enact corporate governance laws, more and more organisations and corporate bodies are seeking assurance that the information assets within organisations are properly protected from security risks and are taking the necessary measures to ensure business continuity. To this end organisations are now adopting and implementing the best practice standards, ISO / IEC 17799. But the question is, to what extent have the information security standards influenced corporate bodies and organisations in Nigeria adopted, implemented and obtained certification to the ISO 17799 standard. It is therefore very important that people and corporate bodies should be a policy guiding information security so as to keep private information confidential and much secured.

V. THE NIGERIAN SITUATION

Nigeria like many other nations in the global village has recently faced numerous challenges following an increased reliance on information technology. Although technological advancements have been of great importance, it cannot be denied that they have been overwhelmed by a number of problems. Information has severally been compromised, leading to serious problems in the corporate sector [9] and confidentiality, veracity, and availability of data have been jeopardized,[10] as cyber criminals in Nigeria have been reportedly been working together to break into organization databases. This scenario calls for a swift modeling of the information security standard for the corporate society in Nigeria to ensured information transfers from one person or organization to another to have a more favorable business environment.

Although automated operations seem to dominate the modern information systems in the corporate sector, there has been rising need to employ sufficient and well trained personnel to detect and respond to threats. Since automated machines can easily be manipulated by unauthorized persons, human power ought to be incorporated in the implementation of data security in the information systems [11]. In 2002, various security analyzers suggested the incorporation of extra elements in the information security systems, including authenticity and possession. Confidentiality has been maintained in the currently used security system since the encryption of personal credit cards and other confidential information have been limited to appear in very few places. This has greatly reduced fraud since various personal codes are not publicly displayed [12]. For instance, according to the 2002 report by Parker, online transactions using credit cards would only involve the displaying of the card data in limited number of places [12]. This would reduce the chances of the number being tracked, reducing the chances of confidentiality breach. By so doing, individual privacy has been increased. Considering the dynamic nature of information systems, regular and frequent testing and reviewing of information system security measures ought to be performed to enhance security. It is highly recommended that the reviewing and the checking of the security systems should be performed by people who were not involved in the development of the security system [12].

On this basis, the compliance of information security measures among businesses in Nigeria can be described as a crucial practice for enhancing safe data transfers within the information network [13].

As reported by [14], the emergence of e-commerce in Nigeria necessitates the establishment of ideal and reliable information security systems among banking institutions. Quite importantly, secure information security roadmap ought to be one of the focal areas of consideration among financial institutions in order to reap the benefits of online transactions. Notably, the reinforcement of information security has been accompanied with ‘no-repudiation’, where each party involved in any financial transaction must fulfill the obligations of the contract, which acts as a guarantee for

ISBN: 978-988-19251-6-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

the clients to indulge into the transaction. In this case, each party involved cannot deny being involved in such a contract. This has lowered chances of any act of fraud since parties cannot breach the contact without a mutual consensus. In this respect therefore, information security has been reinforced to a great extent [11].

According to [15], the security reinforcement of banks with online banking services in Nigeria has greatly helped in the reduction of financial crimes. Previously, over-reliance on paper banking and insecure online transactions culminated in many fraud cases. As it has been reported, people could easily forge documents as well as track online transactions of others to swindle huge amounts of money. Many people have lost lots money due to over-reliance on insecure automated banking systems and manual banking. When information security in online banking was introduced to the country's financial industry, the cases of fraud declined significantly [13]. This was only facilitated through a highly secured system that met international standards, creating minimal chances of losing money through fraud since the automated banking machines are highly encrypted with special data, which can only be provided by account holders for authentication of any transaction.

As noted by [16], security systems in Nigeria should be regularly checked and modified in order to reinstate and maintain the safety of banking using a computerized system. This is on the basis that the currently advancing information technology in education centers is acting as catalyst for new technological inventions. As a result, individuals are developing new techniques of hacking online information which threatens the security employed in the current information systems. Regular tests and adjustments on the current status of information security would be able to reduce any chances of fraudulent activities in the banking industry, with an aim of creating confidence among account holders on the online banking strategy [17]. Encrypting of the processed data should be reinforced with biotech strategy to authenticate users. This strategy seeks to ensure more security in the corporate sector using the internet and avoid any chances of money losses among bank account holders [18].

With the intensive use of new technology in the Nigerian corporate sector, it has been possible to reduce many financial crimes like fraud and forgery in the financial industry. Since most of banking processes are personalized through the encryption of account holders' data, forgery or fraud have not been as common since transactions are processed through an automated system [19]. On this basis, the use of security reinforcement in the online banking system in Nigeria has played a significant role in securing the financial industry [20]. With response to the global trends in the information security, Nigerian systems in the corporate sector must safeguard the intellectual property in both private and public sectors. By so doing, it would be easier to realize significant economic and social growth in the country.

According to [21], a computer crime as well as cyber survey conducted recently indicated that Nigeria is the most internet fraudulent country in Africa. Besides, the same report further stated that the giant of Africa is ranked third among others identified with cyber fraud and computer crime in the world. [21], expressing concerns on how terrorists have been distorting information on internet, said internet facility has recently become an instrument of terrorism. He reiterated that the third world war might be fought on computers as terrorist groups like Al Queada and Boko Haram have been taking advantages of internet facilities to launch attacks and invectives.

This development, he stressed, has called for concerted efforts among stakeholders, civil society groups, corporate bodies and government institutions to join forces together to rid the continent of the imminent terrorist attacks through the use of information technology.

Crime remains elusive and ever strives to hide itself in the face of development. As measures and techniques for detecting crimes and criminals advance, criminals also look for means of hiding from these measures – the Internet currently serve as a hiding place for fraudsters who has simply migrated from the streets to an electronic platform offered by the world wide web; the screens in fig. 5, 6 and 7 below shows these features graphically. Different nations have adopted different strategies to contend with crimes depending on their nature and extent. Certainly, a nation with high incidence of crime cannot grow or develop. That is so because crime is the direct opposite of development. It leaves a negative social and economic consequence [22]. For Nigeria, a nation in the process of saving her face regarding cyber-crimes, efforts are now being directed at the sources and channels through which cybercrimes are being perpetuated – the most popular one being Internet access points.

Majority of the cybercrimes perpetrated in Nigeria generally are targeted at individuals and not necessarily computer systems, hence they require less technical expertise. The damage done manifests itself in the real world. Human weaknesses such as greed and gullibility are generally exploited. The damage dealt is largely psychological and financial. These crimes are similar to theft, and the likes that have existed for many centuries offline even before the development of high-tech equipment. Through the internet, the same criminals or persons with criminal intents have simply been given a tool which increases their potential pool of victims and makes them all the harder to trace and apprehend [23].

One of the surveys that were carried out identified nine information security threats [24]:

- Virus attacks
- Unauthorized access to systems
- Theft of confidential information
- System sabotage
- Internal staff abusing internet access
- Financial fraud through deception
- Theft of computer equipment
- Denial of service attacks
- Unauthorized web site modification

It is therefore recommended that the federal government, in a joint venture with other stakeholders, should doversatile hunt strategy at stopping spam. The federal government should be able to make a law that can prohibit spam and other emerging threats that will affect the safety and security of internet [25].

ISBN: 978-988-19251-6-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

VI. SYSTEM DESIGN AND IMPLEMENTATION

In order to proffer solution to the current information security issues in the country as it concern the transmission of information across networks, the Advanced Encryption Standard (AES) standard is been employed. AES which supersedes DES has been adopted by the U.S. government and is now used worldwide. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data. AES has the following strong features - A private key symmetric block cipher with 128-bit plaintext block, 128/192/256-bit keys; - Stronger & faster than "Triple-DES"; - Active life of 20-30 years; - Efficient in both software and hardware implementations; - Simple in design; - Suitable for smart cards (memory requirement AES was announced by National Institute of Standards and Technology (NIST) as U.S. FIPS PUB 197 (FIPS 197) on November 26, 2001 after a five-year standardization process in which fifteen competing designs were presented and evaluated before it was selected as the most suitable. AES is the first publicly accessible and open cipher approved by the National Security Agency (NSA) for top secret information when used in an NSA approved cryptographic module.

The AES messaging model described is implemented in graphical user interface.

The sequence of the entire process is presented by screens as shown in the figures below.

Fig. 1. Access control window

Fig. 1. Above, grants old users, login access and password reset if required. That is to say, a new user must signup to be able to access the system and send sensitive information across the network. That is similar to the screen below.

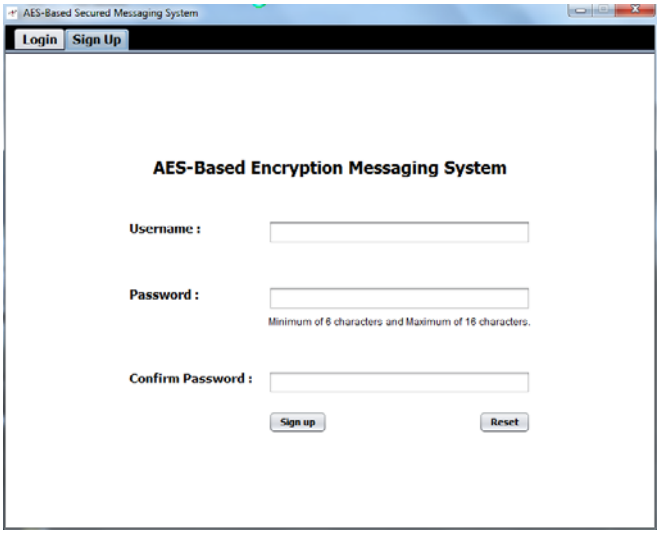

Fig. 2. This screen allows the user of the system to create a unique key to encrypt and decrypt send information or messages sent over the network.

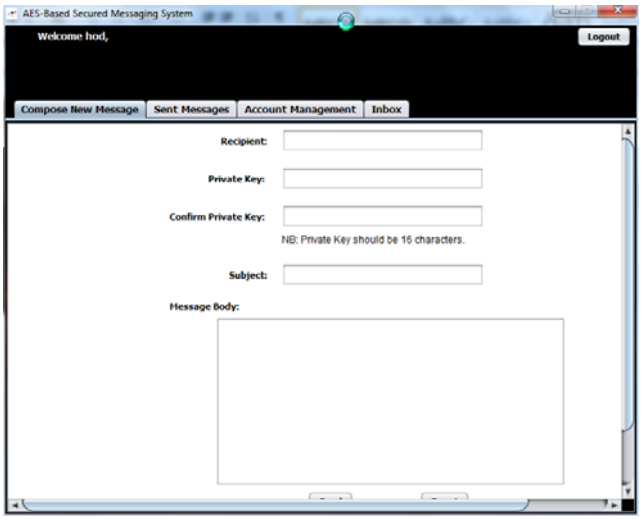

Fig. 3. A screen that gives a valid user of the system access right to create messages, send messages, manage accounts and view all messages in the box.

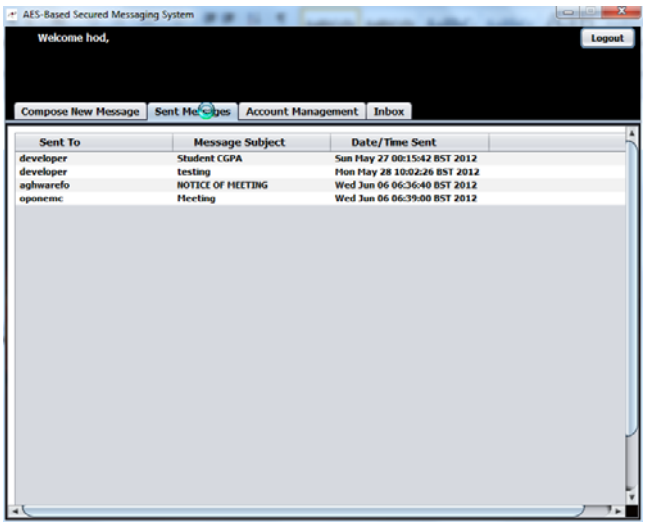

Fig. 4. Messages the user (hod) created and sent to other users of the system.

ISBN: 978-988-19251-6-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

The most interesting part of the system is its ability to encrypt and decrypt information / messages sent across the network using the unique 16 character key. Fig. 5, 6 and 7 below shows these features graphically.

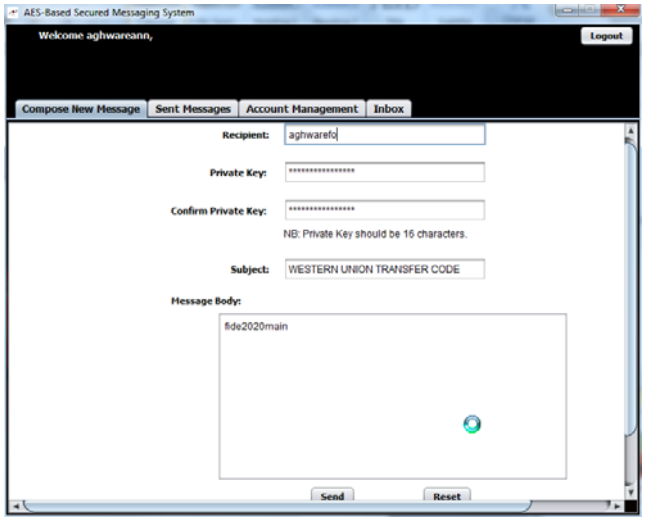

Fig. 5. Encryption screen

Fig. 5. above, shows how, aghwareann use a confirmed private key to create a message which encodes a transfer access to another user (aghwarefo).

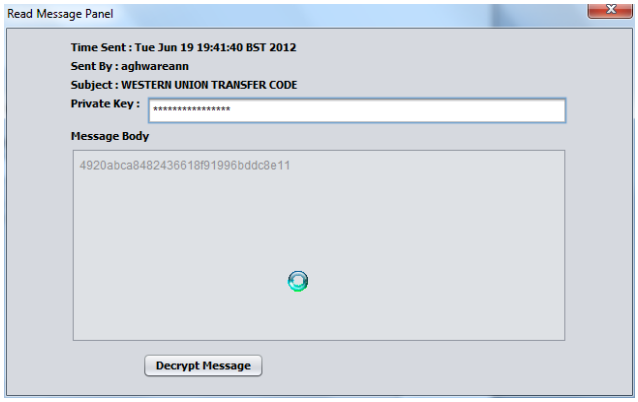

Fig. 6. The encrypted message

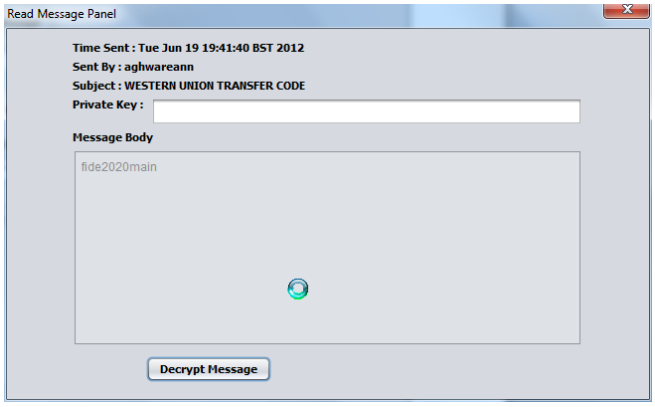

Fig. 7. The decrypted message using the same 16 character private key.

V11. RECOMMENDATIONS AND CONCLUSION

The previous researches over the years have revealed that most of the information breaches and compromised data experienced over networks and the internet are people centred.

The main possible way to solve Information security breaches is through legislative and regulatory measures, this measure will make sure that organization must fulfill their own obligation by providing the appropriate protection of the personal data of their customers, they must also ensure that they reduce the risk of personal data of their customers are not comprised by third party, criminal and even their internal staff. The AES messaging model amongst the other measures is therefore recommended for corporate Nigeria and other corporate organisations that sent information across networks to ensure confidentiality, availability and proper integrity.

REFERENCES

[1] W. Knight, “Hacking Will Cost World $1.6 Trillion This Year”, Z DNet U K. July 2000. Available: http://news.zdnet.co.uk/story/0,,s2080075,00.html
[2] (Computer Security Institute), “Financial Losses Due to Internet Intrusions”, Trade Secret Theft and Other Cyber Crimes Soar, March 2001.[Online]. Available: http://www.gocsi.com/prelea/000321.html
[3] W. Straub, E. Goodman, and R. Baskerville “Information security: policy, processes, and practices”, *Advances in Management Information Systems*, Vol. 11 , US: M.E. Sharpe, 2008.
[4] R. Vacca, “Computer and information security handbook”, *Morgan Kaufmann series in computer security Morgan Kaufmann*, Morgan Kaufmann. 2009.
[5] NIST, *Guide for the Security Certification and Accreditation of Federal Information Technology Systems, Special* Publication 800-37. Information Security Policy Roadmap, 2004. http://www.cmu.edu/iso/governance/policies/information-security-roadmap.html
[6] J. Colley, “*The information security professional is more than “a necessary evil”* 2009. Available: http://www.out-law.com/page-7614
[7] Delloitte “*Global financial Services security Survey”*, 2007. Available: http://www.deloitte.com/
[8] A. Mcllwraith, ,*Information security and employee behavior: how to reduce risk through employee education, training and awareness*, Hampshire: Gower Publishing Company, 2006.
[9] J. Isaca, *The business model for information security*. London: Routldge, 2010.
[10] J. Ozioko, and A. Oji, “The challenges and opportunities of e-Commerce for Nigerian economy”. *Unizik Law Journal*, Vol.4(1), p. 52-76, 2002.
[11] S. Olugbenga, The internet and emergent regulatory legal framework: A selective appraisal. *Modern Practice Journal of Finance & Investment Law*, Vol.2(3), p. 166-181, 2000.
[12] R. Okoinigene, and B. Adekanle, Cybercrime in Nigeria. *Business Intelligence Journal*, Vol. 1(1), p. 93-99, 2009.
[13] S. Brenner, *Law in the era of smart-technology*. Oxford: Oxford University Press, 2007.
[14] K. Kumar, *Cyber laws, international property and e-commerce security*. New Delhi: Dominant Publishers, 2003.
[15] D. Olowu, The road to secure information systems in Nigeria. *Journal of Information Technology*, Vol. 4(3), p.57-71, 2001.
[16] A. Yagba, Information security roadmap in African economies. *Journal of IT & Business Trends*, Vol. 7(1), p. 26-35, 2001.
[17] J. Onyido, Intellectual property protection. *Modus International Law & Business Quarterly*, Vol. 5(2), p.13-27, 2004.
[18] S. Ososami, Information technology and the corporate sector.*Modus International Law and Business Quarterly*, Vol.6(3), p.28-35, 2001.

ISBN: 978-988-19251-6-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

[19] Y. Chung, and M. Yung, *Information security applications: 11th international workshop, WISA 2010.* New York: Prentice Hall, 2011.
[20] A. Olukuyinsola, Anti-fraud systems in the Nigerian banking sector. *Modern Practice Journal of Finance and Investment Law*, Vol. 4(7), p. 113-118, 2000.
[21] M. Ikpehai, Global Computer Crime and Security Survey, Issue 302, 2012.
[22] L. Sylvester,.The Importance of Victimology in Criminal Profiling. 2001. Available: http://isuisse.ifrance.com/emmaf/base/impvic.html.
[23] E. J. Aghatise, "Cyber-crime Definition", Computer Crime Research Center. June, 2006. Available online at: www.crime-research.org
[24] F. Akinsuyi. "The Dawning of Information Security Legislations, What Nigerian Corporations Can Do to Prepare", 2009 [Online] Available: http://www.nigerianmuse.com
[25] Msexchange Exchange Server Anti-Spam Information & News, 2010. [Online] Available: http://antispam.msexchange.org/
[26] L. Schlesinger, Your Biggest Threat. ZDNet: Apr, 2002. [Online]. Available: http://techupdate.zdnet.com/
[27] S. Hinde, "The future for Computer Audit and Security", Information Systems Auditor, Jan. 2000.[Online]. Available: http://www.intnews.com/internal_audit.htm

ISBN: 978-988-19251-6-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)